Claims

1. A method of securely voting over a network, comprising:

delivering an electronic ballot from a server with the vote serial number on the ballot, to an individual;

filling in the ballot and creating a set of ballot choices that are digitally signed using the individual's secret key;

delivering the ballot choices with the individual's electronic signature, and the vote serial number to the server; and

creating a data element from the individual's electronic signature over the ballot choices, the server's electronic signature over the ballot choices and the vote serial number to record the ballot choices in a data store at the server, and retaining the ballot choices as a vote.

2. The method of claim 1 further comprising confirming the retention of the vote at the server by signing the individual's signature of the ballot, the server's signature of the ballot and the vote serial number, and transmitting the signed confirmation to the individual who submitted the ballot.

3. The method of Claim 1, further comprising: recording in the server's data store the server's digital signature of the ballot to allow verification at the server that all of the ballots cast have not been tampered with.

4. The method of claim 3, further comprising: verifying for all individuals voting that none of the ballots have been tampered with by reconstructing the ballot for each individual using the vote serial number, creating a digital signature over each reconstructed ballot by using the server's public key, and verifying the digital signature against the ballot signature using the server's private originally recorded when the individual created and submitted the ballot with the individual's private key and verifying the digital signature against the ballot signature originally recorded when the individual created and submitted the ballot, digitally signed with the individual's private key.

5. The method of claim 2, further comprising: allowing the individual to verify that their ballot is retained in the server's data store accurately reflecting the way it was cast by presenting the confirmation to the server; decomposing the confirmation into the individual's signature of the ballot, the server's signature of the ballot, the vote serial

number and the server's signature which resulted in the confirmation; recomputing the server's signature on the confirmation to ensure the confirmation has not been altered; extracting the vote serial number out of the confirmation if it has been verified that the confirmation has not been altered; and indexing a database in the server to allow reconstruction of the individual's ballot as it was cast.

6. The method of claim 5, further comprising: storing the individual's private encryption key, a certificate for the individual's public key and a voter identification generated when the individual registers with the system on a portable storage device; and reading the information on the portable storage device before allowing a ballot to be cast.

7. The method of claim 6, wherein said portable storage device is a smart card, and further comprising reading the information on the smart card before allowing a ballot to be cast.

8. The method of claim 6 wherein said certificate is an X.509 certificate.

9. The method of claim 1, further comprising: entering demographic data onto the ballot and storing the demographic data in relation to the ballot stored by the server.

10. The method of claim 1, further comprising: creating an election voter table at the server from encrypted individual's voter identification; and comparing each ballot to the encrypted individual's voter identification to detect if an individual attempts to cast more than one ballot.

11. The method of claim 1 wherein said ballot is a bit-map.

12. The method of claim 1 wherein said ballot is an HTML or XML document.

13. A method of securely voting over a network, comprising:

delivering an electronic ballot from a server with the vote serial number on the ballot, to an individual;

filling in the ballot and creating a set of ballot choices that are digitally signed using the individual's secret key;

delivering the ballot choices with the individual's electronic signature, and the vote serial number to the server;

creating a data element from the individual's electronic signature over the ballot choices, the server's electronic signature over the ballot choices and the vote serial number to record the ballot choices in a data store at the server, and retaining the ballot choices as a vote;

confirming the retention of the vote at the server by signing the individual's signature of the ballot, the server's signature of the ballot and the vote serial number;

transmitting the signed confirmation to the individual who submitted the ballot; and

allowing the individual to verify that their ballot is retained in the server's data store accurately reflecting the way it was cast.

14. A method of securely voting over a network, comprising:

delivering an electronic ballot from a server with the vote serial number on the ballot, to an individual;

filling in the ballot and creating a set of ballot choices that are digitally signed using the individual's secret key;

delivering the ballot choices with the individual's electronic signature, and the vote serial number to the server;

creating a data element from the individual's electronic signature over the ballot choices, the server's electronic signature over the ballot choices and the vote serial number to record the ballot choices in a data store at the server, and retaining the ballot choices as a vote;

recording in the server's data store the server's digital signature of the ballot to allow verification at the server that all of the ballots cast have not been tampered with; and

verifying for all individuals voting that none of the ballots have been tampered with.

15. A system for conducting secure voting over a network, comprising:

a server having a data store associated therewith, said server being configured for connection to the network for communicating with terminals connected to the network;

said server being further configured for delivering an electronic ballot having the vote serial number on the ballot, to an individual at a terminal connected to the

network, and said ballot configured for being filled in by an individual, and for having a subset thereof corresponding to the ballot choices delivered to the server with the individual's electronic signature and the vote serial number thereon; and

the server being further configured for receiving the subset of the ballot and creating a data element from the individual's electronic signature over the ballot choices, the server's electronic signature over the ballot choices and the vote serial number to allow recording of the subset of the ballot within the data store and retained therein as a vote.

16. The system of claim 15, wherein: the server is further programmed for confirming retention of the vote at the data store thereof by signing the individual's signature of the ballot, the server's signature of the ballot and the vote serial number, and transmitting the signed confirmation to the individual who submitted the ballot.

17. The system of claim 15, wherein: the server is programmed for recording in the data store the server's digital signature of the ballot for allowing verification at the server that all of the ballots cast have not been tampered with.

18. The system of claim 17, wherein: the server is programmed for verifying for all individuals voting, that none of the ballots have been tampered with, by reconstructing the ballot for each individual using the vote serial number, creating a digital signature over each reconstructed ballot by using the server's public key, and verifying the server's signature over the ballot choices originally recorded when the individual created and submitted the ballot choices.

19. The system of claim 16, wherein: the server is configured for allowing an individual to verify their ballot is retained in the server's data store in a manner accurately reflecting the way it was cast in response to the individual presenting the confirmation to the server; for decomposing the confirmation with the individual's signature of the ballot, the vote serial number and the server's signature which resulted in the confirmation; recomputing the server's signature on the confirmation to ensure the confirmation has not been altered, extracting the vote serial number out of the confirmation if it has been verified that the confirmation has not been altered; and for indexing a database in the server to allow reconstruction of the individual's ballot as it was cast.

20. The system of claim 19, further comprising: a portable storage device configured for connection and transmission of information to the server, said information being an individual's private encryption key, a certificate for the individual's public key and a voter identification number generated when the individual registered to vote through the server; and the server being configured for receiving the voter ID and public key certificate from the portable storage device before allowing a ballot to be cast by the individual.

21. The system of claim 20, wherein: said portable storage device is a smart card, and further comprising a smart card reader connected to the individual's terminal.

22. The system of claim 20, wherein: the server is configured for processing an X.509 certificate, and wherein said certificate on the portable storage device is an X.509 certificate.

23. The system of claim 15, wherein: the server is programmed for generating a ballot which allows input of demographic data and for storing the demographic data in relation to each ballot stored.

24. The system of claim 15, wherein: the server is programmed for creating an election voter table from a one-way hash of individual's voter identification; and for comparing each ballot to the individual's hashed voter identification to detect if an individual attempts to cat more than one ballot.

25. The system of claim 15, wherein said server is programmed to generate said ballot as a bit-map.

26. The system of claim 15 wherein said server is programmed to generate said ballot as an HTML or XML document.

27. A system for conducting secure voting over a network, comprising:

a server having a data store associated therewith, said server being configured for connection to the network for communicating with terminals connected to the network;

said server being further configured for delivering an electronic ballot having the vote serial number on the ballot, to an individual at a terminal connected to the network, and said ballot configured for being filled in by an individual, and for having a

subset thereof corresponding to the ballot choices delivered to the server with the individual's electronic signature and the vote serial number thereon;

the server being further configured for receiving the subset of the ballot and creating a data element from the individual's electronic signature over the ballot choices, the server's electronic signature over the ballot choices and the vote serial number to allow recording of the subset of the ballot within the data store and retained therein as a vote; and

the server being further programmed for confirming retention of the vote at the data store thereof by signing the individual's signature of the ballot, the server's signature of the ballot and the vote serial number, for transmitting the signed confirmation to the individual who submitted the ballot, and for allowing an individual to verify their ballot is retained in the server's data store in a manner accurately reflecting the way it was cast in response to the individual presenting the confirmation to the server.

28. A system for conducting secure voting over a network, comprising:

a server having a data store associated therewith, said server being configured for connection to the network for communicating with terminals connected to the network;

said server being further configured for delivering an electronic ballot having the vote serial number on the ballot, to an individual at a terminal connected to the network, and said ballot configured for being filled in by an individual, and for having a subset thereof corresponding to the ballot choices delivered to the server with the individual's electronic signature and the vote serial number thereon;

the server being further configured for receiving the subset of the ballot and creating a data element from the individual's electronic signature over the ballot choices, the server's electronic signature over the ballot choices and the vote serial number to allow recording of the subset of the ballot within the data store and retained therein as a vote; and

the server being programmed for recording in the data store the server's digital signature of the ballot for verifying at the server that all of the ballots cast have not been tampered with, by reconstructing the ballot for each individual.